Communications of the IIMA

2006

Up from the Ashes: The TippingPoint Technology Case

Bruce A. White
Quinnipiac University

Up from the Ashes: The TippingPoint Technology Case

Bruce A. White
Quinnipiac University, Hamden, CT 06518
Phone: 203.582.3386, Fax: 203.582.8664,
E-mail: bruce.white@quinnipiac.edu

ABSTRACT

In the legend of the Phoenix bird, the bird dies on a fiery pyre, but arises from the ashes. This is a case that parallels that legend. It's a case showing a technology company that almost died, but came back stronger. As NetPliance, it developed and marketed a "thin client," bare-bones Internet Appliance in the Business to Consumer B2C area. As the reorganized TippingPoint Technologies, it has become a leader in the intrusion prevention system area, using hardware and networking technologies in the Business to Business environment. Instead of just detecting viruses, spam, spyware and other negative attacks that have already passed through the firewall, their product detects and proactively stops the intrusion as they enter the network.

Keywords: Network security, intrusion prevention systems (IPS), technology success factors

PROLOGUE

Sunday January 30, 2000

John McHale didn't know whether to laugh or cry. He had just watched his company's first (and only) ad at the XXXIV Superbowl. The ad was great – it featured the Dallas Cowboy's cheerleaders – skimpy outfits and all – promoting his company's product. The company had entered into the marketing agreement on July 30, 1999 – when NetPliance's future was rosy – and it looked like NetPliance would be the Microsoft or Dell of the future. Unfortunately, on this Superbowl Sunday, six months later, it looked like that great ad, costing over $2 million dollars was going to suck some of the remaining funds from a quickly dying company.

This case is what happened to that company and how it might be a lesson for IT students.

ORGANIZATIONAL BACKGROUND

John McHale was CEO of NetPliance, with headquarters in Austin Texas. He had a background as a technology and networking entrepreneur. In 1996, he (with others) sold Networth to Compaq Computers. He (and others) then organized NetSpeed, an end-to-end DSL system. In March 1998, McHale and crew sold NetSpeed to Cisco for about $250 million in stock. Then in 1999, McHale started another technology company – NetPliance. In this case, we'll learn how NetPliance was transformed into TippingPoint Technologies, a network security leader, and how TippingPoint became a unit of 3Com.

Setting the Stage

In the turbulent technology world of 1999, it seemed like every consumer in the United States wanted to connect to the internet. Dot com startups were plentiful. Venture capitalists seemed willing to throw money at any new web enterprise, and consumers wanted to get online.

NetPliance created an "internet appliance". Basically this was a bare bones computer without a hard drive, but very affordable at $300 and able to get consumers onto the internet quickly and at a bargain prices as compared to traditional desktop computer systems at four to five times as much money. Their model was called the iOpener. With McHale and staff, NetPliance had strength in computer hardware with an understanding of networking and internetworking.

The iOpener was similar to other internet appliances, such as the eVilla by Sony and the Audrey by 3Com, the iPAQ by Compaq, and others.

From a website (http://www.adamlotz.com/iopener.html), the author noted:

> *"The Iopener is a nifty little computer built by Netpliance. It is essentially an "internet terminal,"*
> *a compact and attractive 10" LCD monitor with a complete computer built into the enclosure. It is*
> *cheap, silent, energy efficient, and has a small footprint. It's the "kitchen counter" internet*
> *appliance that geeks the world over have been looking for.*
>
> *Why the hype? It sells for $99. No kidding. But there's a catch - Netpliance designed the system to*
> *work solely with their ISP service, which is priced at a reasonable $22 a month. A modem is built*
> *in to the unit, and the software that comes with it is well done - the first time you turn it on and*
> *plug your modem in, it will "phone home" and let you set up an account."*

Using a QNX real-time operating system, the iOpener had no hard drive, no major application software (like the Microsoft Office suite), and was truly, just a device to use in connecting to the Internet. This bare-bones nature was one of the downfalls as consumers soon found that they could not create word processing documents or spreadsheets, or even to download such files that may have been attached to e-mail messages. Users were limited to surfing the internet and sending e-mail

After a successful IPO (initial public offering of stock), the market quickly changed. Consumers found that an internet appliance wasn't robust enough for their tastes, and the demand for them took a nosedive. The Audrey by 3Com lasted six months; the eVilla by Sony lasted about five months. Adding to the problem was a massive downturn in capital spending among telecommunications service providers – ILEC (incumbent local exchange carriers) and CLEC (competitive local exchange carriers). The iOpener was caught between consumers wanting more and telecommunications entities not enhancing services.

The boom quickly became bust as far as NetPliance was concerned. In November 2000, NetPliance cut their staff by 38%. And just over a year after the Superbowl ad, on February 2, 2001, they cut the remaining staff by 54%. This was over 70% of the staff gone in four months. Staff that remained looked around wondering if they would be the next to go. The purging even caused them to move to smaller quarters, and the perks from the heyday of NetPliance's earlier successes also died.

CASE DESCRIPTION

The stock that once was valued at $18 in the IPO was now too low to be listed on the NASDAQ markets. Times were desperate for John McHale and the NetPliance crew.

The quickest way to remain in business was to reorganize. The company did a 15 to 1 reverse stock split (so the stock could remain listed on NASDAQ) and become TippingPoint Technologies. They had created a little breathing space – but the next issue John McHale and the remaining staff faced was "what is TippingPoint Technologies going to do"? The expertise brought by McHale, Kip McClanahan, Kent Savage and others from their days together at NetSpeed, was in computing hardware and networking. What products and services could they bring to the marketplace? An early (but aborted) focus was to deliver "premium service over broadband networks". Once bitten by the whims of the consumer market, could the reorganized TippingPoint Technologies go back into the field selling premium products to consumers?

On September 11, 2001, terrorists attacked three times in the United States – twice at the World Trade Center in Manhattan and once at the Pentagon in Washington DC. This national disaster was part of the impetus driving TippingPoint technology to consider network security as a possible strength. With skills in computer hardware, knowledge of networking and data communications (and with a great deal of internal soul-searching), TippingPoint changed focus to the "business to business" market, and left the consumer marketplace. They introduced the UnityOne™ - as "advanced hardware-based network security solutions that can integrate and interlock firewall, intrusion detection and vulnerability assessment functionality into a single high-speed appliance" (TippingPoint press releases 2002). With business networks receiving gigabits of information each second, a fast device to test each packet and to shuttle viruses and undesirable traffic was needed. But, developing market share and profitability were not quickly achieved. With a new product and a new market, cash and cash equivalents fell (see chart):

Cash and cash equivalents (Millions)
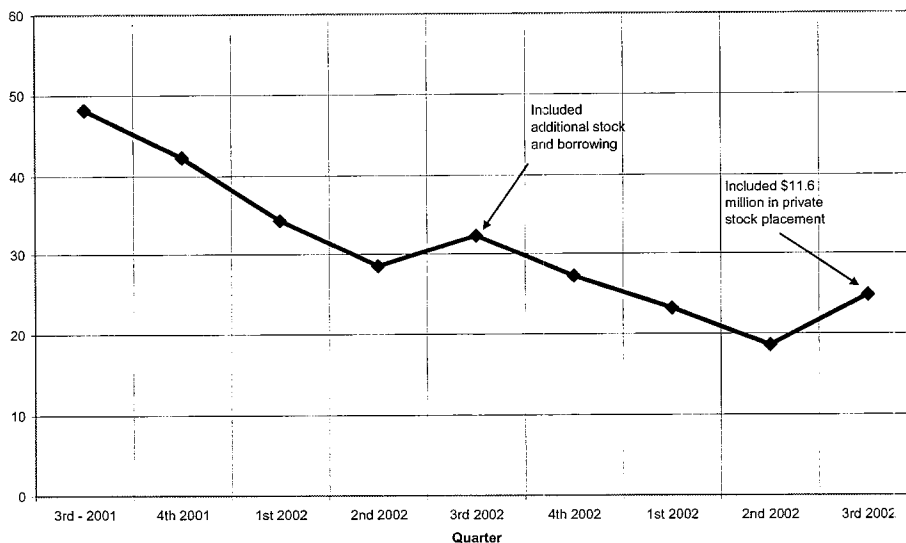
Even with a smaller payroll costs continued. People had to get paid to develop the new product line, the research and development had to continue. Sales were slow in coming. Companies had to be convinced that the new TippingPoint had viable products and services.

Slowly, TippingPoint worked at getting their point across. Their focus had changed from selling small devices to consumers to selling larger (and much more complex and profitable) devices to businesses. Marketing was different -- and it was a new market niche. As businesses moved to electronic commerce, business-to-business commerce, and business to consumer commerce, the transmission of electronic data greatly increased. But as businesses now had a greater reliance on electronic transactions there was also a greater exposure to risks. Viruses, intrusions, denial of services as well as spam and spyware regularly consumed a sizable portion of the corporate bandwidth.

TippingPoint looked to a device that sat on the incoming data stream, just inside the firewall. This hardware and software device was much more robust than the localized desktop software packages like Symantec, McAfee and Norton Utilities. By sitting on the main incoming line, everything in (and out) of a company could be scrutinized. With powerful, high speed hardware devices, incoming mail messages and data could be scanned with negative elements screened out. As an "intrusion prevention system" (IPS), the combination hardware / software solution went beyond detecting viruses, it stopped them as they entered the corporate network system. The PC desktop software virus packages did protect individual PC systems, but lacked the scalability of testing gigabits of information each second. [Note: McAfee recently acquired the IntruShield package to expand from the desktop virus protection field into the IPS field.] An intrusion could be considered whenever any undesired event occurs. In the networking area, such intrusions might be viruses, denial of service attacks, spam, phishing, spyware and other negative communications.

Most end-user computer systems use desktop software systems to detect and clean viruses from their systems. Such packages are marketed by Symantec, McAfee, and Norton as "anti-virus" software. As such, the end user must update his or her system and periodically run a system scan.

Intrusion prevention systems are hardware and software solutions on a more robust (and complex) level. As such, the TippingPoint solution is built onto high speed devices just inside the networking firewall. As a hardware solution, the device needs to function at gigabit speeds to extremely quickly analyze incoming data packets, and to screen out harmful elements. An analogy between intrusion detection and intrusion prevention systems might be to notice that you have a bug in your kitchen (detection), or have a chemical barrier around your house that stops such bugs from even reaching the house or kitchen (prevention). TippingPoint's products serve as such intrusion prevention devices as compared to the desktop software packages that serve as intrusion prevention systems.

TippingPoint had to overcome existing *intrusion detection systems* (IDS) with the advanced *intrusion prevention systems* (IPS). IDS systems detected possible intrusion activities, but were plagued by 'false positives' (i.e. events / messages that were not intrusions, but were detected as possibly intrusions) and by their lack of speed (inability to handle gigabits detection. Although a new category (IPS) had been created, competitors claimed that TippingPoint was just using a marketing ploy by changing *detection* into *prevention*.

With the volume of data that passes into networks, the hardware devices must be very fast – or the network traffic would be slowed down. TippingPoint offers products tailored for a company's bandwidth needs. Their latest product, named the M60, is designed to function at 60 gigabits-per-second. This system "utilizes a state-of-the-art hybrid approach, with a combination of anomaly filters, SYN proxy, rate shaping and statistical techniques to protect against Denial of Service and Distributed Denial of Service attacks" (TippingPoint press releases, 2006). This speed of process was remarkably different than the slower IDS systems.

The UnityOne™ line of products now include what is billed as the "Zero Day Initiative" – a process to recognize new viruses and intrusions as quickly as possible. In their press releases, they state: "The Digital Vaccine Service ensures evergreen protection against emerging threats [...] rogue applications like Peer-to-Peer and Instant Messaging from running rampant throughout the network." It has been recognized as an industry leader by the Gartner Group.

MEDIA REPORTS

Slowly in an attempt to reach customers, TippingPoint worked with the technology media to demonstrate and impress. Tim Greene wrote in Network World in February 2002 that: "Start-up TippingPoint Technologies last week introduced a new type of device that identifies intrusion attempts at blazing speeds and automatically blocks them, unlike traditional intrusion-detection software that detects attacks but requires human intervention to ward them off. UnityOne devices can take the place of firewalls, intrusion-detection appliances, vulnerability-assessment servers and VPN gateways, saving customers 65% off buying the equipment separately."

A press release on February 25, 2003 stated that TippingPoint's UnityOne line "were awarded The Tolly Group's 'UP TO SPEC' certification in the first true network-based intrusion prevention product evaluation based on performance and security precision. UnityOne appliances and systems are the first network-based intrusion prevention products to receive third-party certification". The press release went on to state: "all Unity One appliances blocked 100 percent of attacks tested with complete accuracy (no false positives, no false negatives)." (TippingPoint press releases 2003).

Slowly the company started to get noticed. George Hulme, writing in Information Week in March 2003 noted: "Security vendor Tipping Point Technologies Inc. last week revealed several network-based intrusion-prevention appliances that the company says can stop worms, viruses, and denial-of-service attacks. TippingPoint's UnityOne-400, -1200, and -2400 devices work at speeds of 400 Mbps, 1.2 Gbps, and 2.4 Gbps, respectively. The appliances can support more than 1 million concurrent sessions and 25,000 new sessions per second, the vendor says."

In an article in Optimize in October 2003, Thomas Danford stated about an installation of the TippingPoint UnityOne system at the University of Dayton: "Last December, the university installed TippingPoint Technologies Inc.'s UnityOne Intrusion Prevention Appliance, a high-speed device that blocks malicious traffic at gigabit speeds and incorporates peer-to-peer piracy-prevention capabilities. The university now prevents more than a million network threats every month, including worms and viruses, using this technology."

AWARDS AND RECOGNITION

Also in October 2003, TippingPoint was honored with the "Best New Product" award by the Canadian Technology Industry Association. (TippingPoint press release). They were also awarded the NSS "Gold Award" for intrusion prevention on January 19, 2004. The NSS Group is described as "the world's foremost network and security testing organization".

Other awards and recognition include:
- SC Magazine Awards 2006
- Best Corporate Appliance Security Solution 2005

- Frost & Sullivan 2005 Award for Technology Leadership 2005
- Frost & Sullivan Market Penetration Leadership Award - IDS/IPS Market 2005
- Aberdeen Group - Best Practices Award for Security 2005
- Info Security Products Guide - Best Deployment Scenario 2005
- SC Global Awards 2005 - Principal Awards - Best Security Solution
- Frost and Sullivan 2005 Network Security Infrastructure Protection Entrepreneurial Company of the Year 2005
- TechWorld Network Awards 2005

By third quarter 2003, TippingPoint Technologies showed a slight profit – after three years of declining cash balances. Their stock shares were at $15 in August 2003, and climbed through early December. In December 2003, they announced that 3Com had made an offer to acquire them for $47 a share. In January 2004, TippingPoint was acquired by 3Com, and made a subsidiary of 3Com.

ENJOYING SUCCESS

While watching Superbowl XXXIX in 2005, John McHale and his friends looked out of his window overlooking Lake Austin and relaxed, enjoying the fruits of their labors. With luck (both good and bad), a terrorist attack, and a decimated staff, he was able to work a "miracle". From the ashes of a failed internet appliance company, TippingPoint had arisen, like the fabled Phoenix. John had taken the $47 a share offer from 3Com and left TippingPoint. Where he will resurface in the future is unknown, but at the time, he can watch the video of the NetPliance Superbowl ad from 2000 and have the last laugh.


CURRENT CHALLENGES/PROBLEMS FACING THE ORGANIZATION

Many of the other NetPliance / TippingPoint Technology staff remained when TippingPoint became part of 3Com. 3Com has been a networking technology company, but has lost market share to Cisco, Juniper Networks (and others) in the past ten years. With the acquisition of TippingPoint and a smaller Voice over Internet Protocol (VoIP) company, 3Com is attempting to regain lost customers by providing increasing services and innovations. 3Com can temporarily claim a competitive advantage with integrated networking, security and VoIP products. In the dynamic world of computing, it may be a short lived advantage as Cisco and others bring their solutions to the marketplace. If TippingPoint can continue to introduce faster-and-faster IPS devices to the marketplace, as well as integrate their technology with parent 3Com's switches and equipment, they may be able to retain that competitive advantage. Media reports also point to TippingPoint developing the IPS logic to be implemented on 3Com switches and routers. That integration of security and intrusion protection with switches could also help sustain a longer competitive advantage over Cisco (until Cisco duplicates the technology, that is).

Technology continues to move forward. The famous "Moore's Law", promoted by Gordon Moore, co-founder on Intel has become a "self-fulfilling prophesy" – even in the eyes of Dr. Moore. Chip makers and computer companies continue to improve the techniques and develop faster and faster devices. Such increases in technology are also a threat to 3Com and TippingPoint. They must continue to roll out faster switches and faster intrusion prevention systems or lose their competitive advantage. The M60 at 60 gigabits per second might be fast today, but in a year will become average and after that – out-dated and slow.

A market can only bear so many entrants. Michael Porter's five forces model (Supplier Power, Buyers Power, Barriers to entry, Threat of Substitutes, and Rivalry) can help us understand TippingPoint's position. Intrusion prevention can become a crowed market, and companies like Tipping Point will need to establish a sustainable competitive advantage to remain competitive. But they will also need to find ways to differentiate themselves so as avoid the substitution threat, and also make up of the opportunity in this early stage of the technology to use their competitive advantage to create barriers to entry for the competition. Building on the Porters five forces model, their partnership with 3COM gives them buyer power and greatly lessens the suppliers' power. They have collaborated with Symantec on enterprise security systems – with TippingPoint's intrusion prevention system and Symantec's Security Management System, which should help keep Symantec from direct competition. They are in an excellent position right now to be a top player in the intrusion prevention market, but need to hang on to the competitive advantage and be mindful of the forces as notated by Porter. Just as they had to battle the slower, in-adequate IDS systems to create the genre of IPS, now they have to look at the marketplace for competition (rivals), and alternative

systems (potential substitutions). Their hardware platform is able to run at very high speeds and when coupled with their software solutions, is able to diagnose threats and intrusions.
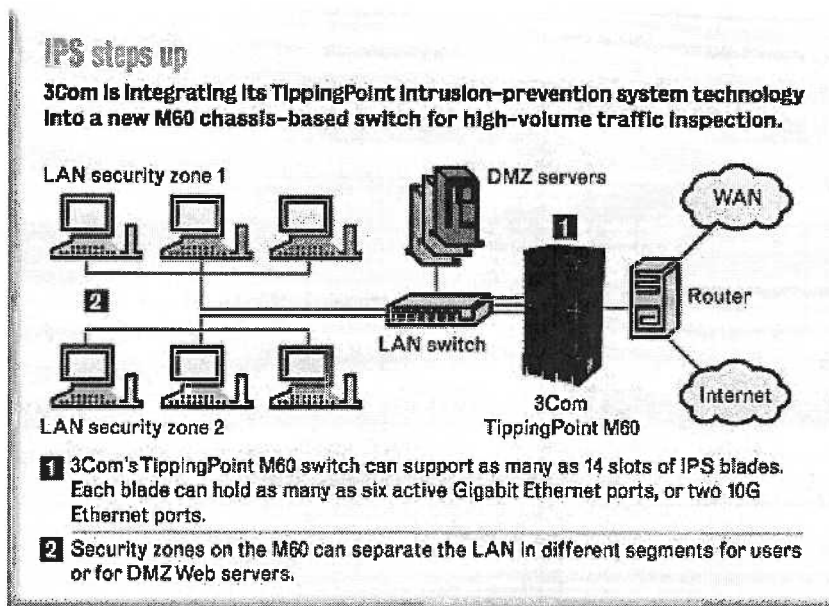
In the fragile world of security and intrusion prevention, every day can bring a new threat. It might happen that a new and unique virus could arrive on the technology scene any day – and if the UnityOne™ fails to catch it, competitors may gain in the competitive race. At this stage, their proactive model seems to be effective, but a major failure could give competitors enough ammunition to attack.

SUMMARY

NetPliance found that the internet appliance marketplace quickly changed from a viable business model to a failing business model. Consumer whims can (and did) change, as well as factors in the telecommunication capital improvement arena. Reorganizing as TippingPoint technologies, and using their staff that had strengths in hardware and networking, they created a strong intrusion prevention system and had to overcome the slower, and sometime inadequate intrusion detection systems. With being acquired by 3Com, they find the synergy of a networking, router and switch company (3Com) combined with a networking security company (TippingPoint) gives them a competitive edge. Whether they can sustain that competitive advantage is the big question before 3Com and TippingPoint – and only time can tell.

As expressed in the opening comment, TippingPoint Technologies were able to "arise from the ashes" of the failed NetPliance to be a leader in the network security area. Innovation, staying close to corporate strengths (hardware / networking), tenacity and some luck made the difference.

REFERENCES

Anonymous, (2002), Austin America-Statesman: Plugged In Column, Austin American-Statesman, February 18, 2002.

Anonymous, (2001), Netpliance Relabels (becomes TippingPoint Technologies), Interactive Week, August 20, 2001, vol. 8, issue 32, page 38

Anonymous, (2001), Smart Thinking: Internet Appliance Market to Double by 2005, Printed Circuit Fabrication, July 2001, Vol. 24, Issue 7, page 6

Anonymous, (2001), What is an Internet Appliance? <u>Electronic Engineering</u>, July 2001, page 7.

Boulton, Clint, (2001), Netpliance: At Half Staff, <u>Internetnews.com</u>, February 2, 2001, (retrieved March 26, 2005)

Brull, Steven V. (2000), Gateway's Big Gamble; Ted Waitt is building the IT Department for the Masses, <u>Business Week</u>, June 5, 2000, pg EB 26

Danford, Thomas (2003), Learning to protect a network, <u>Optimize</u>, October 2003, page 74.

Davis, Jim, (200), Netpliance raises $144 million in IPO, <u>CNET</u>, March 17, 2000, retrieved from http://news.com.com/2100-1040-238127.html?legacy=cnet on March 25, 2005.

Dreazen, Yochi (2003), Workplace Security (A Special Report): The Sky is Falling? Software and tech-security companies are sounding the warning – and hoping to profit from the fears, <u>Wall Street Journal</u> (Eastern edition), September 29, 2003, page R.4

Dreyfuss, Joel (2000), Want to go online? This appliance can take you there, <u>Fortune</u>, Jan 10, 2000, vol. 121, issue 1; pages 177-178

English, David, (2001), Compaq iPaq Home Internet Appliance A-1 <u>Fortune</u>, Summer 2001.Vol.143, Iss. 13; pg. 137

Fratto, Mike, (2002), Tipping the Scales, <u>Network Computing</u>, September 30, 2002, Vol. 13, Issue 20, 2 pages.

Gartner Group (2006), http://mediaproducts.gartner.com/reprints/3com/133189.html, retrieved February 23, 2006

Goldsborough, Reid, (2000) Personal computing: Is the PC dead?, <u>Link-Up</u>, Nov/Dec 2000, Vol. 17, Issue 6; Page 9

Greene, Tim (2002), Streamlining Intrusion Detection, <u>Network World</u>, vol. 19, Issue 8, page 10, February 25, 2002

Hulme, George (2003), Tipping the Security Scales, <u>Information Week</u>, March 3, 2003, issue 929, page 69

Jason, Leila (2001), E-Business: Simple PCs Can Help Speed Elderly Onto Net, <u>Wall Street Journal</u>, July 16, 2001, pg. B.5

Kranhold, Kathryn, (2000), The Real Action: Ad Bowl XXXIV – This Year's Lin-up Features A Heavy Blitz of Dot-Coms and Some Odd Cowboys, <u>Wall Street Journal</u>, January 28, 2000, page B.1

Laswell, Matthew, (2006), Personal Interview.

Lawton, George (2001), Internet Appliances Struggle for Acceptance, <u>Computer</u>, July 2001, vol. 34, Issue 7, page 12

Lewis, Peter H. (2001), Pulling the Plug on home Internet Appliances, <u>Fortune</u>, April 16, 2001, vol. 143, page 436

Lotz, Adam, Adam's Guide to the Iopener, http://www.adamlotz.com/iopener.html (retrieved March 25, 2005)

Net Economy, (2006), http://www.findarticles.com/p/articles/mi_zdtne/is_200201/ai_ziff21617#continue, retrieved February 23, 2006.

Piazza, Peter, (2003), Faith in intrusion prevention, <u>Security Management</u>, October 2003, vol. 47, issue 10, page 28

Taulli, Tom, (2000), Netpliance: Internet with Training Wheels, <u>Internetnews.com</u>, March 15, 2000, (retrieved March 26, 2005)

3Com website, (2006), http://www.3Com.com , (retrieved frequently)

TippingPoint Technology website: http://www.tippingpoint.com, (retrieved frequently)

TippingPoint Technology Press Release (2001), various press releases, (retrieved from: http://www.tippingpoint.com/pdf/press/2001/ on March 26, 2005)

TippingPoint Technology Press Release (2002), various press releases, (retrieved from: http://www.tippingpoint.com/pdf/press/2002/ on March 26, 2005)

TippingPoint Technology Press Release (2003), various press releases, (retrieved from: http://www.tippingpoint.com/pdf/press/2003/ on March 26, 2005)

TippingPoint Technology Press Release (2004), various press releases, (retrieved from: http://www.tippingpoint.com/pdf/press/2004/ on March 26, 2005)

Wasserman, Todd (2000), 'Meet Audrey' says 3Com in TV Ads, marking a new day for Web devices, <u>Brandweek</u>, November 27, 2000, page 5

Wildstrom, Stephen H. (2001), The Best Net Machine Isn't Good Enough; The eVilla offers a great screen and software, but it's huge, slow, and too Sony-centric, <u>Business Week</u>. July 30, 2001, Iss. 3743; pg. 19

Yandel, Fauve, (2001), EarthLink Agrees to Buy Netpliance Subscribers, <u>Internetnews.com</u>, February 28, 2001, (retrieved March 26, 2005)

Zizzo, Thomas, (2001), Comeback predicted for Internet Appliances, <u>Electronic Business</u>, May 2001, vol. 27, Issue 5; page 44.